

Claims

What is claimed is:

1. A method for using a first financial instrument to facilitate access to a second financial instrument, comprising the steps of:

identifying a method of authentication for facilitating the activation of the first financial instrument;

verifying the method of authentication is valid for the first financial instrument;

using the first financial instrument to facilitate the verification that the method of authentication allows access to a second financial instrument; and

allowing access to the second financial instrument.

2. The method of claim 1,

wherein the first financial instrument includes at least one of a credit card, a smart card, a stored value card, a stored value product, a personal digital assistant, a cellular telephone, an electronic traveler's check, an on-line financial service, a radio frequency enabled payment device, and an automated teller machine; and

wherein the second financial instrument includes at least one of a credit card, a smart card, a stored value card, a stored value product, a personal digital assistant, a cellular telephone, an electronic traveler's check, an on-line financial service, a radio frequency enabled payment device, and an automated teller machine.

3. The method of claim 1, wherein the first financial instrument includes a smart card and the second financial instrument includes an on-line financial service, and further comprising the step of using the smart card to identify the method of authentication to include smart card and PIN for accessing the on-line financial service.

4. The method of claim 1, wherein the method of authentication includes at least one of user identification and password, a user identification and pass-phrase, biometrics, a smart card and PIN, a smart card and digital certificate, a palm pilot and digital certificate, sound verification, radio frequency and password, radio frequency and biometrics, infrared and biometrics, and infrared and password.

5. A method for using a first financial instrument to facilitate access to a second financial instrument, comprising the steps of:

identifying a method of authentication for facilitating the activation of the first financial instrument;

using the first financial instrument to facilitate the authentication of a user in connection with accessing a second financial instrument; and

allowing access to the second financial instrument based on the authentication of the user.

6. The method of claim 5:

wherein the first financial instrument includes at least one of a credit card, a smart card, a stored value card, a stored value product, a personal digital assistant, a cellular telephone, an electronic traveler's check, an on-line financial service, a radio frequency enabled payment device, and an automated teller machine;

wherein the second financial instrument includes at least one of a credit card, a smart card, a stored value card, a stored value product, a personal digital assistant, a cellular telephone, an electronic traveler's check, an on-line financial service, a radio frequency enabled payment device, and an automated teller machine; and

wherein the method of authentication includes at least one of user identification and password, a user identification and pass-phrase, biometrics, a smart card and PIN, a smart

card and digital certificate, a palm pilot and digital certificate, sound verification, radio frequency and password, radio frequency and biometrics, infrared and biometrics, and infrared and password.

7. A method for facilitating the selection of one authentication method for accessing a plurality of financial instruments, comprising the steps of:

identifying an authentication method for facilitating access to a first financial instrument;

verifying that the authentication method can be used to facilitate access to a second financial instrument; and

using the authentication method to facilitate access to both the first and second financial instruments.

8. The method of claim 7, further comprising the steps of:

configuring the first financial instrument to include a smart card; and

configuring the second financial instrument to include a brokerage account, wherein the smart card may be used to access the brokerage account.

9. A method for using a first restricted service to facilitate authentication of a user in connection with accessing a second restricted service, comprising the steps of:

identifying a level of security for facilitating the authentication of a first restricted service;

verifying that the level of security for authentication of the first restricted service may be used to facilitate authentication of a second restricted service; and

using the authentication of the first restricted service to facilitate access to the second restricted service.

10. The method of claim 9, wherein the level of security for authentication includes at least one of user identification and password, a user identification and passphrase, biometrics, a smart card and PIN, a smart card and digital certificate, a palm pilot and digital certificate, sound verification, radio frequency and password, radio frequency and biometrics, infrared and biometrics, and infrared and password.

11. A method for using a first restricted service to facilitate the authentication of a user for accessing a second restricted service, comprising the steps of:

checking for a cookie residing on a user's computing unit, wherein a host reads the preference set in the cookie;

identifying the method of authentication of the first restricted service based on the preference set in the cookie;

selecting a minimum level of security for facilitating authentication of the first restricted service, if the preference set does not include information regarding the minimum level of security for authentication of the first restricted service; and

using the first restricted service to authenticate the user in connection with accessing the second restricted service using the minimum level of security for authentication.

12. A method for using a first financial instrument to facilitate access to a second financial instrument, comprising the steps of:

requesting data in connection with the first financial instrument via a web server;

receiving data in connection with the first financial instrument via the web server, wherein the data includes information regarding the authentication method for accessing the first financial instrument;

transmitting the data having information regarding the authentication method for the first financial instrument from the web server to a security server; and

using the first financial instrument to facilitate access to the second financial instrument by transmitting the data from the web server and the security server to an external security store via a communication channel and receiving data from the external security store via the communication channel.

13. A computer implemented method for using a first financial instrument to facilitate access to a second financial instrument, comprising the steps of:

obtaining data on the first financial instrument via a communication channel coupled to a computer system having a memory and a processor;

storing the data in the memory and using the processor to configure the data for allowing the first financial instrument to authenticate a user in connection with accessing the second financial instrument; and

allowing access to the second financial instrument upon using the first financial instrument to authenticate the user.

14. A communication system using a first financial instrument to facilitate access to a second financial instrument, comprising:

a host server for processing data in connection with a first financial instrument;

a database coupled to the host server for collecting data on the first financial instrument where the data includes information in connection with an authentication method for using the first financial instrument; and

a communication channel coupled between the host server, the database, the first financial instrument, and the second financial instrument for transmitting at least a portion of the data from the host server and the first financial instrument to the second financial

instrument in order to authenticate the second financial instrument.

15. The communication system of claim 14,

wherein the first financial instrument includes at least one of a credit card, a smart card, a stored value card, a stored value product, a personal digital assistant, a cellular telephone, an electronic traveler's check, an on-line financial service, a radio frequency enabled payment device, and an automated teller machine;

wherein the second financial instrument includes at least one of a credit card, a smart card, a stored value card, a stored value product, a personal digital assistant, a cellular telephone, an electronic traveler's check, an on-line financial service, a radio frequency enabled payment device, and an automated teller machine; and

wherein the authentication method includes at least one of user identification and password, a user identification and pass-phrase, biometrics, a smart card and PIN, a smart card and digital certificate, a palm pilot and digital certificate, sound verification, radio frequency and password, radio frequency and biometrics, infrared and biometrics, and infrared and password.

16. A communication system using a first financial instrument to facilitate access to a second financial instrument, comprising:

a database for receiving data from the first financial instrument;

a processor coupled to the database for configuring the data in a format;

a communication channel in communication with the database and the processor for transmitting the data from the first financial instrument to the database and the processor, wherein the data includes a method of authentication for the first financial instrument; and

using the data to authenticate the second financial instrument upon transmitting the data to the database and processor.

17. The communication system of claim 16,

wherein the first financial instrument includes at least one of a credit card, a smart card, a stored value card, a stored value product, a personal digital assistant, a cellular telephone, an electronic traveler's check, an on-line financial service, a radio frequency enabled payment device, and an automated teller machine;

wherein the second financial instrument includes at least one of a credit card, a smart card, a stored value card, a stored value product, a personal digital assistant, a cellular telephone, an electronic traveler's check, an on-line financial service, a radio frequency enabled payment device, and an automated teller machine; and

wherein the method of authentication includes at least one of user identification and password, a user identification and pass-phrase, biometrics, a smart card and PIN, a smart card and digital certificate, a palm pilot and digital certificate, sound verification, radio frequency and password, radio frequency and biometrics, infrared and biometrics, and infrared and password.

18. A communication system using a first financial instrument to facilitate access to a second financial instrument, comprising:

a host server including a processor for processing data in connection with the first financial instrument;

a memory coupled to the processor for storing the data;

an input digitizer coupled to the memory and the processor for inputting the data into the memory; and

an application program stored in the memory and accessible by the processor for directing processing of the data by the processor, wherein the application program is configured to facilitate the steps of:

identify a method of authentication for activating the first financial instrument;
verify the method of authentication is valid for the first financial instrument;
use the first financial instrument to verify that the method of authentication allows
access to a second financial instrument; and
allow access to the second financial instrument.

19. A communication system using a first financial instrument to facilitate
access to a second financial instrument, comprising:

a browser for submitting data to a web server, wherein the browser and the web
server communicate via a communication channel and the data submitted to the web server
includes information in connection with the first financial instrument's minimum level of
security for authentication;

a security server coupled to the web server via a second communication channel for
retrieving data from the web server in connection with the minimum level of security for
authentication; and

a database coupled to the security server via a third communication channel for
receiving, storing, and submitting data to and from the security server, wherein the browser,
web server, security server, and database communicate in order to authenticate the second
financial instrument using the first financial instrument's minimum level of security for
authentication.

20. The communication system of claim 19,

wherein the first financial instrument includes at least one of a credit card, a smart
card, a stored value card, a stored value product, a personal digital assistant, a cellular
telephone, an electronic traveler's check, an on-line financial service, a radio frequency
enabled payment device, and an automated teller machine;

wherein the second financial instrument includes at least one of a credit card, a smart card, a stored value card, a stored value product, a personal digital assistant, a cellular telephone, an electronic traveler's check, an on-line financial service, a radio frequency enabled payment device, and an automated teller machine; and

wherein the minimum level of security for authentication includes at least one of user identification and password, a user identification and pass-phrase, biometrics, a smart card and PIN, a smart card and digital certificate, a palm pilot and digital certificate, sound verification, radio frequency and password, radio frequency and biometrics, infrared and biometrics, and infrared and password.